© 2019 IJSRSET | Volume 6 | Issue 2 | Print ISSN: 2395-1990 | Online ISSN : 2394-4099
Themed Section : Engineering and Technology
DOI : 10.32628/IJSRSET1962161

A Study on Secrecy Preserving Multi-keyword Matching Technique on Cloud for Encrypted Data

Priti Kakade[1], Prof. Pragati Patil[2]

[1]PG Scholar, Department of Computer Science Engineering, Abha-Gaikwad Patil College of Engineering, Nagpur, Maharashtra, India.

[2]Assistant Professor, Department of Computer Science Engineering, Abha-Gaikwad Patil College of Engineering, Nagpur, Maharashtra, India.

ABSTRACT

This paper provides data privacy in cloud in encrypted form. And that encrypted data searching through fuzzy technique. Multi-keyword fuzzy search can afford the misspelling which lead to larger index file scan and higher index complexity. This scheme is secure, efficient and accurate because of novel multi-keyword fuzzy search scheme by exploiting the locality Sensitive Hashing (LSH) technique. Fuzzy matching is performed through search algorithm design.

Keywords : Cloud Computing, Searchable Encryption, Privacy-Preserving, Fuzzy Keyword Search, Ranked Index.

I. INTRODUCTION

Cloud computing is the large storage technology of the internet. In this paper, data owner opt to encrypt their sensitive data like health records, banking records etc before outsourcing it to cloud and maintain the secrecy through the decryption key to the authorized users. This technique is very helpful to the authorized users to search the sensitive data's. This scheme make a challenging problem for example ,in order to search a relevant document among encrypted data set stored in the cloud, due to the large volume of data, that the users apparently impractical to download or decrypt the entire dataset.

For searching on the encrypted data is effective and efficient mechanism. Early work consider only word by word search and some last work has been built by and search by the secure index. It also is a secured work but it support only word by word search and support only single keyword search only. At last they built in to the capability to multiple keyword searches. This also supports the exact keyword matching. When the user type misspelled word in the searching time output will not match, then finally updated the capability to fuzzy. This form can accept the misspelled keyword and give the accurate result. This paper support multi-keyword search and it will run the algorithm in multiple rounds.

The advanced data structure are used to represent the searchable index and efficient search algorithm, that run over corresponding data structure, design of cryptographic protocols are maintained the data security and data privacy. This paper consist of a system model in which to outsource a set of files to the cloud server, the data owner builds a searchable index which is secure for the file set and then uploads the encrypted files, along with the index, to the cloud server. To search over the encrypted files, an authorized user first obtains the trapdoor which is the “encrypted” search keyword(s), from the data owner, the trapdoor is submitted to the cloud server. Upon receiving the trapdoor, the cloud server executed the search algorithm over the indexes and returns the matched files to the user as the search result. The following figure shows the architecture of encrypted data in cloud [6].

This paper considers two threat models depending on the information available to the cloud server.

- Known Ciphertext Model: Only the encrypted document, searchable index and encrypted query all which are outsource from data owner are available to cloud server. And protect plain text from cloud server.
- Known Background Model: Here user has a pre idea about the document that is given by data owner.

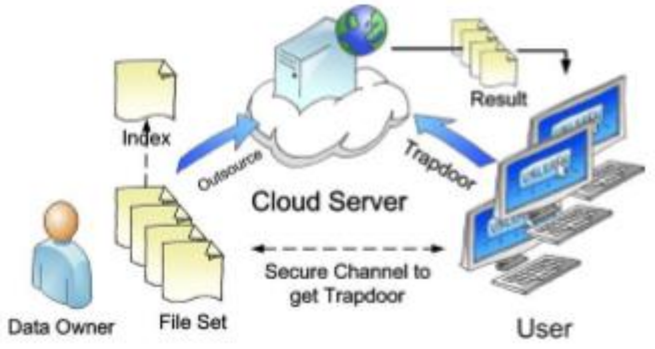

Figure 1 : System architecture of search over encrypted data in cloud computing

This paper achieving the multi-keyword fuzzy search and no need of pre defined dictionary. We achieve this by several novel design based on locality sensitive hashing (LSH) and bloom filter. By using LSH this scheme find the document with matching keyword efficiently. Maintain the security problem by using the cryptographic protocol and ensure the security problem, which give efficient and accurate result.

II. LITERATURE REVIEW

Dawn Xiaodong Song David Wagner Adrian Perrig [1] has proposed a method cryptographic scheme for the problem of searching for encrypted data and give proofs of security for the resulting crypto systems. These techniques provide different crucial advantages. They provide secrecy and privacy for encryption, such that it sense the untrusted server does not have any knowledge about the plaintext when only given the ciphertext than the search result. Controlled searching is used, that the untrusted server cannot search for an randomly chosen word without the user's permission. Hidden queries are supported, so that the user asks the untrusted server to make search of secret word without showing the word to the server. The algorithms present are simple, fast and introduce almost less space and communication issue, and hence are practical to use today.

Previous work shows how to build file which is encrypted and and secure mail servers, but must have to sacrifice functionality to ensure security. In this paper, it shows how to support searching process without any loss of data privacy. The encryption and searching algorithms need O(n) number of stream cipher and block cipher operations. There are two types of approaches. One way is to build up an index that, for each word of interest, lists the documents that include the word .An alternative is to perform a sequential scan without an index. When the documents are large advantage of using an index is faster than the sequential scan. The disadvantage of using an index is that keeping and makes changes in the index. So the method of using an index is more suitable for mostly-read-only data. These papers introduce solution for searching with sequential scan and start with scheme and show that encryption algorithm provides provable secrecy.

Wenhai Sun, Bing Wang, Ning, Ming Li, Wenjing Lou, Y. Thomas Hou [2] In this paper, present a privacy-preserving multi-keyword text search (MTS) scheme with similar-keyword-based ranking to address this problem. To support multi-keyword search and result of ranking depending on search, it is propose to build the search index based on term frequency and the vector space model included cosine similarity measure to attain high search result accuracy.

To protect the sensitive data before outsourcing to cloud service providers (CSPs) usually enforce users, data security through processes such as firewalls and virtualization. These mechanisms do not protect users' privacy from the CSP itself since the CSP possesses full control of the hardware of the system and low levels of software stack. Cosine measure in the vector space model is a state-of-the-art similarity measure commonly used in plaintext information retrieval community. This paper provides accuracy "improved multi-keyword ranked search, security". Tree based search algorithm is used in this scheme.

Ning Cao, C.Wang, Ming Li, K.Ren, and Wenjing Lou [3]. In this paper, for the first time, we define and make solution for the challenging problem of privacy-preserving multi-keyword ranked search over encrypted data in cloud computing (MRSE). The term coordinate matching is used i.e., as many matches as possible, to capture the relevance of data documents to make query search. Basic idea for the MRSE is proposed and it is based on secure inner product computing, and then introduced two significantly improved MRSE schemes to achieve various stringent privacy requirements in two different threat models. To protect privacy of data and unsolicited accesses in the cloud and beyond, sensitive data, for example, e-mails, health records of a person, photo albums, tax documents, financial transactions, and so on, have the data owners to be encrypted before outsourcing to the commercial public cloud. To meet the effective data retrieval that is needed, the large amount of documents on cloud server is obtained by relevance ranking, instead of providing undifferentiated results. Such type of ranked search system enables data users to find the most relevant information more quickly, than searching for unnecessary data. Ranked search can also eliminate unnecessary network traffic and send only the most ranked data, which is highly important. To improve the user searching experience, the ranking system support multiple keywords search. The existing paper is still not adequate to provide users with acceptable result ranking functionality. In this paper it will search for multiple keywords and index is provided for the keyword. During the index construction, each document is accompanied with a binary where each bit represents whether corresponding keyword is contained in the document. Thorough analysis investigating privacy and efficiency guarantees of the proposed schemes is provided, and make experiments on the real-world data .MRSE system consists of four algorithms as "set up, trapdoor, query, built index," for multi-keyword ranked search.

Cong Wang, Ning Cao, Kui Ren, and Wenjing Lou, [4]. In this paper, they define and solve the problem of privacy preserved ranked keyword search over cloud data which is encrypted. Ranked search provide only relevant data rather than of sending unnecessary results, and further ensures the file retrieval accuracy. Before data's are outsourcing to cloud server. In Cloud Computing, data owners may share their data which is outsourced to cloud with a large number of users, who want to retrieve certain specific data files they are interested. The most common ways to perform search through keyword-based. Such type of search technique allows users to selectively retrieve files of interest and has been widely applied in plaintext search scenarios. Lacking of effective mechanisms to ensure the file retrieval accuracy is a significant disadvantage of existing schemes. To attain design goals with privacy it is propose to bring the advance of both crypto and IR community to design (RSSE) scheme that is the ranked searchable symmetric encryption, in the spirit of "as strong-as-possible" security guarantee. This paper define the problem of secure ranked keyword search over encrypted cloud data, and give an efficient protocol, which fulfills the secure and search the functionality with small relevance score information leakage against keyword privacy. This paper investigate the practical considerations and enhancements of ranked search , including the efficient support of dynamics relevance score, the authentication of ranked depending search results, and the reversibility of proposed system include one to-many order-preserving mapping technique. our system design should achieve the following security and performance guarantee 1) Ranked keyword search, 2) Security guarantee, 3) Efficiency. Our ranked searchable encryption system can be made from these four algorithms in two phases, Setup and Retrieval. The proposed solution is efficient and preserving privacy, while correctly resulting the goal of ranked keyword search.

Ming Li, Shucheng Yu1, Kui Ren, and Wenjing Lou [5]. In this paper, we propose a novel framework for access control of PHRs which is present with in the cloud computing based environment. To enable fine grained and scalable access control for PHRs, we use (ABE) techniques that are attribute based encryption to encrypt each patient's PHR data. A PHR service allows a patient to manage, create, maintain and control their personal health data in a centralized place that can access through the web, from anywhere and at any time (if an internet connection is available), which has made to keep the data in the server, accessing and sharing of the medical information more rapidly and securely. Each and every patient has the full control over their individual medical related data's and share their health data with a wide different number of users, such as staffs from healthcare providers, and their family members or friends which the particular patient want to share with. In this way, the accuracy and quality of care that is given to the patient can be improved, and the cost for health caring is low. The providers of PHR can shift their PHR storage and application services into the cloud server in order to lower down their operational cost. Cloud computing is an open platform; the servers are facing the threat to outside attackers. To deal with such risks of privacy exposure, instead of letting the PHR Service as in original form the providers will encrypt patients' recorded, PHR services should give patients (PHR owners) to have control over the selective sharing of their own PHR. Finally, the PHR data should be kept in encrypted format to access control provided by the server. Each patient shall generate her own decryption keys and distribute them to their authorized users. Also they will choose in a fine-grained way which users can have the right to access for which parts of their PHR. To avoid high complexity on key management for each owner and user and then system should be divided into multiple security domains (SDs), where everyone is associated with a subset of all the users. This paper utilize multi-authority based encryption to encrypt the PHR data in a different format, so that patients will give the permission to access not only by personal users, but users from many other public domains with different roles and qualifications.

III. CONCLUSION

We proposed an integrated several innovative design to solve the fuzzy search problems. This paper approach LSH function in bloom filter to construct file index for efficiently search using fuzzy keyword. Here I use different algorithm for keyword search and cryptographic protocol for data privacy and data security.

IV. REFERENCES

[1]. D. Song, D. Wagner, and A. Perrig, "Practical techniques for searches on encrypted data," S&P 2000, vol. 8, pp. 44–55, 2000.

[2]. W. Sun, B. Wang, N. Cao, M. Li, W. Lou, T. Hou, and H. Li, "Privacy preserving multi-keyword text search in the cloud supporting similarity based ranking," in ASIACCS 2013, May 2013.

[3]. N. Cao, C. Wang, M. Li, K. Ren, and W. Lou, "Privacy-preserving multi-keyword ranked search over encrypted cloud data," INFOCOM 2011, pp. 829–837, 2011.

[4]. C. Wang, N. Cao, J. Li, K. Ren, and W. Lou, “Secure ranked keyword search over encrypted cloud data,” ICDCS 2010, pp. 253–262, 2010.

[5]. M. Li, S. Yu, K. Ren, and W. Lou, “Securing personal health records in cloud computing: Patient-centric and fine-grained data access control in multi-owner settings,” in Secure Comm 2010, Singapore, September 7-9 2010.

[6]. Privacy-Preserving Multi-Keyword Fuzzy Search over Encrypted Data in the Cloud Bing Wang Shucheng Yu Wenjing LouY. Thomas Hou, Virginia Polytechnic Institute and State University, Blacksburg, VA, USA University of Arkansas, Little Rock, AR, USA

[7]. W. Sun, B. Wang, N. Cao, M. Li, W. Lou, Y. T. Hou, and H. Li, ”Privacy-preserving multi-keyword text search in the cloud supporting similarity-based ranking,” in Proc. ASIACCS, Hangzhou, China, 2013, pp. 71-82.

[8]. R. X. Li, Z. Y. Xu, W. S. Kang, K. C. Yow, and C. Z. Xu, Efficient multi-keyword ranked query over encrypted data in cloud computing, Futur. Gener. Comp. Syst., vol. 30, pp. 179-190, Jan. 2014.

[9]. Gurdeep Kaur, Poonam Nandal, “Ranking Algorithm of Web Documents using Ontology”, IOSR Journal of Computer Engineering (IOSR-JCE) eISSN: 2278-0661, p- ISSN: 2278-8727Volume 16, Issue 3, Ver. VIII (May-Jun. 2014), PP 52-55

[10]. Qin Liuy, Guojun Wangyz, and Jie Wuz, ”Secure and privacy preserving keyword searching for cloud storage services”, ELSEVIER Journal of Network and computer Applications, March 2011

[11]. Cong Wang et al., ”Enabling Secure and Efficient Ranked Keyword Search over Outsourced Cloud Data”, IEEE Transactions on parallel and distributed systems, vol. 23, no. 8, August 2012

[12]. International Journal of Computer Applications (0975 –887) Volume 126 – No.14, September 2015

[13]. Wenhai Sun et al., "Privacy-Preserving Multikeyword Text Search in the Cloud Supporting Similarity-based Ranking'', the 8th ACM Symposium on Information, Computer and Communications Security, Hangzhou, China, May 2013.

[14]. Jiadi Yu, Peng Lu, Yanmin Zhu, Guangtao Xue,Member, IEEE Computer Society, and Minglu Li,”Toward Secure Multikeyword Top k Retrieval over Encrypted Cloud Data”, IEEE Journal of Theoretical and Applied Information Technology 10th August 2014.

[15]. Ning Cao et al.,” Privacy-Preserving MultiKeyword Ranked Search over Encrypted Cloud Data”, IEEE Transactions on parallel and distributed systems, vol. 25, no. 1, jan 2014

Cite this article as :

Priti Kakade, Prof. Pragati Patil, "A Study on Secrecy Preserving Multi-keyword Matching Technique on Cloud for Encrypted Data ", International Journal of Scientific Research in Science, Engineering and Technology (IJSRSET), Online ISSN : 2394-4099, Print ISSN : 2395-1990, Volume 6 Issue 2, pp. 566-570, March-April 2019.
Journal URL : http://ijsrset.com/IJSRSET1962161